Chapter 3 - Investigating digital crime

Book Section

3

Investigating Digital Crime

Ian Kennedy

Digital forensics is a relatively recent addition to the forensics family and, for this reason alone, the terminology used is undergoing constant definition and redefinition. An increasing number of books are available with titles that make reference to terms such as 'cyberforensics', 'computer forensics', 'Windows forensics' and 'Intrusion forensics'. As we shall see throughout this chapter, not only is the terminology in a state of development but the training and accreditation is changing too.

Hi-tech crime is often associated with computers and especially with the investigation of paedophiles, whilst this may reflect the current caseload of many law enforcement high-tech (or hi-tech) crime units around the UK, it is becoming increasingly common for digital devices other than personal computers to be either the target of a crime, or to be used to assist in the commission of a crime. Mobile phones, digital cameras, personal data assistants (PDAs), mp3 players, and even online storage are currently the technologies of choice for the technically savvy criminal. Digital forensics therefore, extends beyond the confines of the computer and encompasses a broad range of digital technology.

Investigating Digital Crime Edited by Robin Bryant and Sarah Bryant

Evidence and intelligence in digital crime

Robin Bryant

Evidence and intelligence are both forms of information that may be used in an enquiry and a subsequent prosecution.

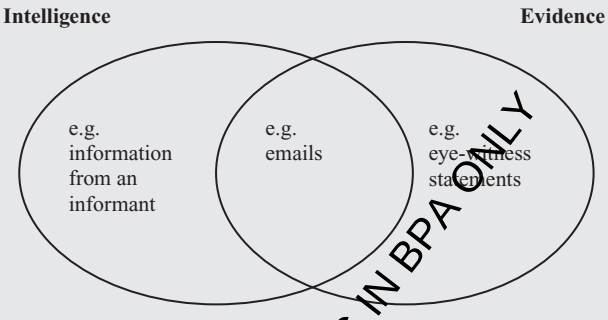

Figure 3.1 Intelligence and evidence

Intelligence is information which, when analysed and interpreted, is of potential value in progressing an enquiry into an alleged, suspected or actual crime. Information from a paid informant for example might constitute intelligence. Evidence, in comparison, is any information which may be of value to a court in deciding on the issues presented to them, most fundamentally on the guilt or innocence of the accused. For a digital crime, recovered parts of an email communication might constitute intelligence and evidence. Not all intelligence will be used as evidence (for example, a recovered deleted SMS communication may suggest a certain line of enquiry), and not all evidence is intelligence (for example, a statement that a witness makes in court). Legislation in the UK governing the collection of intelligence and evidence is extensive.

There are many potential sources of digital crime evidence and intelligence, and some are shown in tables 3.1 and 3.2 below. One unusual requirement for the work of a forensic digital investigator is a broad familiarity with technology, both ancient and modern. For example it is perfectly feasible that a criminal has continued to use his or her reliable Amstrad PCW word-processor to this day. For this reason, police high tech crime units sometimes include impressive repositories of knowledge about defunct computer and

word processing equipment. Many types of office and domestic electrical equipment contain digital memory, and at least some may provide intelligence or even evidence to support an investigation. The list in table 3.1 (below) reflects the wide range of equipment that may be used by offenders.

Table 3.1 Sources of digital information

Sources	Examples
Hard drives	'Winchester' drives, tape drives, IDE drives (2.5 inch, 3.5 inch, 5.25 inch), SCSI drives, ATA drives, DMA drives and external drives.
Discs, tapes, cartridges and pens	Floppy discs (relatively common 3.5in, less common 4.5in, 5.25in); Zip drive cartridges; Jaz drive cartridges; tapes for external tape drives; CD (including miniCD); DVD (including miniDVD, HDDVD, Blu-ray); USB flashdrives (pens or memory sticks).
Network devices, modems and routers	Servers; Network Interface (NIC) cards; internal, external, PCMIA card modems; routers (including wireless routers). Also included under this heading would be the associated software e.g. the configuration file for a home modem/router.
Memory cards	Used in a variety of devices, including digital cameras and laptops. Memory cards include Memory Sticks, Multimedia Cards (MMC), CompactFlash (CF), SmartMedia and Secure Digital (SD, miniSD).
Computer access control devices	These devices include stripe (swipe) cards, dongles, smartcards, keycards, fingerprint recognition pads. Most are a combination of hardware with software. These devices may elicit information concerning the users of the devices.
Volatile memory	Dumped RAM (including passwords and passphrases), state of open network connections.
Personal media players	Included here are 'Walkmans' (cassette, minidisc and CD), mp3 players, multimedia players (e.g. an Archos). Some of these devices (such as an mp3 player) can also save non-music data such as image files.
Recording machines (sound)	Tape machines include: • reel-to-reel tape machines; • cassette recorders players (tapes in C30, C45 and C60 sizes); • answer machines (smaller tape cassettes); • hand held recorders. Some of these machines may have been used to record data (e.g. from a Sinclair Spectrum). CD players/recorders.

Table 3.1 (*Continued*)

Sources	Examples
Digital cameras and camcorders	As well as the images themselves (with date stamps etc.), digital camera memory is also normally able to store other forms of data.
Recording machines (linked to TVs)	VHS video players/recorders. DVD players/recorders (a DVD player may be used to show digital photographs from a USB pen).
Mobile phones, electronic organisers, PDAs and smart devices	Including numerous mobile phone makes; Psion, iPAQ, Apple Newton, Palm Pilot, Blackberry, Trio and i-phone. Pagers, although no longer used by the public in the UK, might still contain useful contact information.
GPS devices	Including GPS devices within cars and hand-held devices (including within mobile phones).
Office equipment	'Telex' machines, fax machines, scanners, printers, photocopiers may all have residual memory information.
Games consoles	NES, SNES, Playstation etc. For example a 'chipped' Microsoft Xbox may have been set up as an ftp server, or a games console may have been used to take part in a chat room.
TV and radio	Digital TVs, digital satellite TV receivers, digital radios
White goods	Microwave cookers and washing machines.
Others	Digital clocks and watches.

3.1 Digital evidence

Quite apart from the legal position on digital evidence, conveying the significance of the evidence itself to the court presents a particular challenge. It is not enough to simply translate technical data into layman's terms as one might translate a foreign language into English. The technical complexity of such cases frequently surpasses the technical knowledge and experience of the court. Some items of evidence may simply seem intangible to a court due to their 'virtual' nature or their confusing similarity to other items of evidence. For example, consider trying to explain the difference between the last access date and the last modified date on an NTFS file system.

Thus, unlike a written document, raw computer evidence must be presented alongside an accurate interpretation which clearly identifies its significance in the context of where it was found. For example, the hard disk of a computer contains raw binary data, and ignoring more complex data types, this may be encoded as

simple binary, binary coded decimal or as hexadecimal data. The value encoded may represent a numeric, alphanumeric, date/time or logical value. Even dates and times can be encoded in a number of ways employing, for example, a 'big endian' or 'little endian' approach in terms of representation.

The interpretation of evidence must be undertaken by a suitably qualified person and then presented in an accessible form for perusal by a court. Over simplification is dangerous as it could lead to the data becoming open to interpretation. Any doubt as to the interpretation of a single item of evidence can often be addressed by correlating it with other evidence such as log files, internet history, and link files.

Unlike some conventional crime scenes, the very existence of evidence may not be obvious to the 'first responder' (the first person to arrive) at a digital crime scene. It is not likely that there will be easily identifiable items of evidence such as footprints or bloodstains to be identified and preserved. Conventional forensics follows the ethos of Locard's exchange principle as described by Thornton (1997); namely 'Every contact leaves a trace'. Akin to evidence such as DNA, digital evidence is also fragile and easily contaminated or damaged. Every click of the mouse could potentially alter data stored on a device and thus destroy vital evidence. Thus, a first responder must not switch on a computer, or 'have a look around' on a machine that is already running, as this threatens the integrity of the evidence contained on the computer, which integrity was debased recently (BBC, 2007g) by a Special Branch detective who breached standard police procedure when he switched on a laptop computer and explored its contents (for over an hour) prior to passing it over to a forensic computer analyst for examination.

Digital forensic investigation in context

Robin Bryant

For a digital forensic investigation to be successful, several different perspectives need to be taken into account, and the three most important considerations are shown in figure 3.2.

For example, examining the image of a SIM card from a mobile phone cannot be regarded as simply a scientific process (the Scientific Disciplines perspective). The examination is taking place because of an investigation (the Law Enforcement perspective) with all that follows from this; possibly in order to corroborate an account for the purpose of furthering an enquiry.

For the enquiry to lead to a successful prosecution, the perspective of the Criminal Justice System (and in particular, the CPS) must also be considered e.g. ACPO principles must have been adhered to, particularly in relation to evidential requirements.

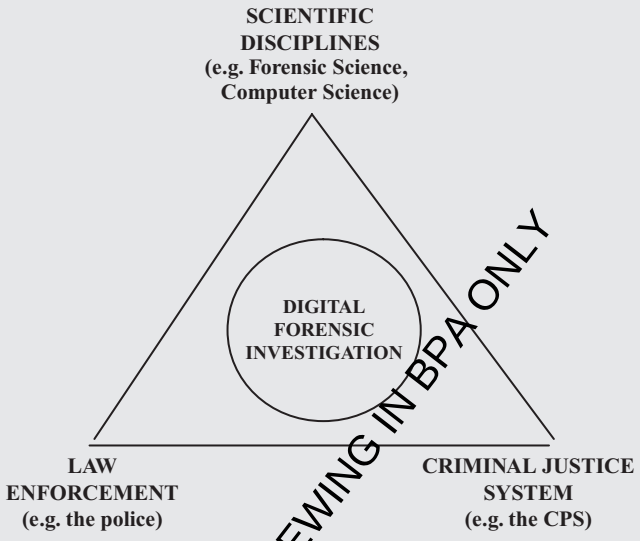

Figure 3.2 Factors impinging on a digital forensic investigation

3.2 How a digital device becomes involved in a crime

Although many crimes committed with the use of a computer may seem to be quite modern, they often include a number of features that may be somewhat more traditional in nature. Using eBay, for example, to offer goods for sale, receive payment and then fail to supply the goods to the customer is essentially a traditional fraud; an old crime committed using a high tech method. Aspects of the same offence can be committed using a newspaper advert or even a handshake with an exchange of cash in the local pub. It is debated elsewhere in this book just how 'new' these forms of criminality really are.

Not all crimes committed using a digital device use it simply as a means to an end. A denial of service (DoS) attack on a website, or the intentional distribution of a virus designed to manipulate data stored on a victim's computer are both

examples of crimes in which the computer itself is the target of the crime; the computer has not simply been used in the commission of the offence.

There are numerous ways in which a digital device may feature within a crime. Some particular examples are discussed in this section.

3.2.1 Fraud and identity theft

The Advance Fee or '419' fraud is a popular confidence trick frequently perpetrated by West African organised crime networks. The 419 reference is taken from the section of the Nigerian Criminal Code relating to Fraud (International Centre for Nigerian Law, 2007). It is a particularly old form of attempted fraud that dates back to the 16th century when it was known as the 'Spanish Prisoner' scam, but its commission is most certainly facilitated through the use of digital technology. Put simply, the scam involves a victim being offered a large sum of money, but in order to access this money the victim must pay a fee in advance. The reasons cited for this are varied but one example is to pay some form of tax to an organisation holding the money. Further requests for payment are then subsequently made until the victim realises what is happening at which point the scammer stops all correspondence and disappears. Figure 3.3 shows a more subtle variant of this scam; a request for money is likely to follow shortly!

Phishing is another modern twist on an old crime. Contacting victims electronically via email, the scammers use social engineering techniques, and masquerade as a legitimate organisation. The organisations of choice are currently eBay, PayPal and certain high street banks. In a recent high profile attack the website Monster.com had a number of its recruiter accounts compromised, and these accounts were then used to log in and obtain the personal details of candidates. Candidate data was then uploaded to a remote server whcih eventually held over 1.6 million entries (Symantec Corporation, 2007a) containing personal information belonging to several hundred thousand candidates, mainly based in the US, who had posted their résumés to the Monster.com website.

Typically, the potential phishing victim is sent an email purportedly from the legitimate organisation with a link to its website that, when visited, superficially looks genuine. The victim is then asked to log in to 'verify' their security details. In some cases additional details such as credit card and corresponding PIN numbers are also requested. Manipulating people into divulging confidential information in this way is more of a problem than one might presume. Dhamija *et al.* (2006) recently completed a study that showed 40 per cent of a test group failed to spot phishing sites while the most sophisticated site fooled 90 per cent of the group.

Hello, dear friend!

My name is Ekaterina. I am 26 years old. I'm from Russia, city Cheboksary.
I live together with my mum and I work as adviser on sale home appliances.
I have many various hobbies: sport, a photo, drawing. I dream to have strong and happy family.
It's my purpose in life. I want to be happy and to do happy my family.
Recently I thought that I have it already. However.....
I wish to tell you history which have pushed me write to you.
6-7 months ago I have got acquainted with man from your country.
His name is Peter. Our meeting was at a seminar in city St.Peterburg.
It was the working meeting. Between us began the novel.
It was so fast and I thought that it's my man. Through 3 days he has left
home. We have understood that letters can not replace our meeting face to face again.
Peter has told that I should arrive to him!!! I was very glad during that moment. I wrote the application for reception visa. I waited reception = visa approximately half of year.
All this time Peter called and wrote to me letters. All things was very good. I have received the invitation from the ambassador for reception =sa. My director has given me holiday from work and I have gone to Moscow to receive visa.
I said this good news to Peter, but he told that he does not want our meeting. He played with me. He has told me that he has wife with 3!!!! children and now he don't want our meeting. I have been broken...
I could not think that it was game with my feelings..... I did not think that people are so severe....
Now I am in Moscow and waiting for reception visa.
I don't want that all was gone for nothing and will be glad if my visa will be useful to our meeting.
I could arrive already in 7-8 days, but I have problem. I don't know any man who would like my arrival.
I hope that it will not sound silly if I will ask you about our meeting and good time together...
I don't know your ideas about my letter, but it would be fine if we could meet and have some weeks or months together.
I want to use my visa for trip to your country and search man with which I would like to have happy and strong family.
I was never married and have no any children. I'm woman which ready to creation family with good man.
I don't know about you anything, but I want it very much.
It would be fine if we could meet, to do friendship or more than simply friendship.
I will be happy if you also have a free time and we could meet soon.
I don't know about your plans at present time, but I sincerely hope that we can have meeting with you in the near future.
You can write all that you want. Ask any questions which interest you.
I hope that you understand my English I began to study English approximately 1,5 year ago. Write to me back and I will tell more about myself and send my photos.

Please, write to me back and send your photos on my regular e-mail: katykitten@bk.ru

Have a good day,
Ekaterina

Figure 3.3 A variant of the 419 scam

As noted in an earlier chapter of this book, the recently updated Fraud Act 2006 includes an amendment to Section 2, fraud by false representation. The Explanatory Notes (Great Britain. Office of Public Sector Information, 2006) state that anyone engaging in the act of phishing is guilty of fraud by false representation.

Using phishing techniques to obtain confidential information has recently led to a number of cases of identity theft. This is the practice of using personal details from another person to open bank accounts, and obtain credit cards, loans, state benefits and documents such as passports and driving licences in a victim's name.

Recent cases include a woman who impersonated her sister's identity to obtain a mortgage (BBC, 2007f), a university tutor who stole nearly £20 000 on two credit cards he had taken out in the name of his former landlords (BBC, 2007h) and a

man who headed a £2.3m identity theft ring targeting the bank accounts of a vicar, businessmen and even the dead (BBC, 2007b). Garlik (2007) recently published a report indicating that during 2006 there were 92 000 cases of reported online identity theft and, it was claimed that 40 per cent of these were committed online. A recent report by security firm Symantec (2007b) indicated that its software alone had been used to block 12.5 million phishing emails per day over the first six months of 2007.

3.2.2 Computer misuse

For computer misuse offences, both the offence and the method used to commission the offence involve computers. The Computer Misuse Act 1990 was established to legislate against offenders who gain unauthorised access to computer systems, possibly with intent to commit further offences or modify any data contained on the target computer system. This is discussed in more detail in Chapter 2.

Computer misuse offences include:

- accessing areas of a competitor's website without authorisation and downloading a large amount of internal information;
- sending a large number (millions) of emails to a former employer's email server causing a system crash, known as a Denial of Service or 'DoS' attack;
- writing and distributing computer viruses and inciting others to spread computer viruses.

There were 144 500 reported cases of computer misuse (excluding malware) alone during 2006, and it has been estimated that over 6 000 000 unreported malware incidents are likely to have occurred in the same year (Garlik, 2007) Malware is discussed in more detail in Chapter 4.

Another area of emerging computer crime is that of an offender connecting to a victim's wi-fi connection without permission. A recent case reported by the BBC (2007d) highlights that such dishonesty in obtaining free internet access is an offence under the Communications Act 2003 and a potential breach of the Computer Misuse Act 1990. This type of activity is discussed in more detail in Chapter 8.

3.2.3 Sexual offences

It has been estimated that some 850 000 sexual approaches are likely to have been made to children over the internet during 2006 (Garlik, 2007). Such offences are found to occur primarily as a result of an offender visiting searching and/or browsing websites, newsgroups or peer to peer networks. The receipt (and in some cases distribution) of email and media such as CD-ROMs may also constitute an offence. In some cases webcam technology has been used in combination with grooming to make an indecent image of a child.

Grooming is the act of an adult communicating with a child with the intention of meeting with the child to commit a further, often sexual, offence. O'Connell (2007) identifies five stages of the grooming process:

1. *Friendship*. In this initial stage flattery is used by the adult to encourage the child into talking in a private chatroom where they will be isolated. It is common for a non-sexual picture of the child to be requested.

2. *Forming a relationship*. The child is asked what problems they have. This creates the illusion of the adult being their best friend.

3. *Risk assessment*. To assess the risk of being detected the adult will at this stage often ask the child about the location of their computer and who else has access to it.

4. *Exclusivity*. With the friendship and risk level established, the groomer then embarks on a process of building up a sense of mutual love and trust with the child. A sense of complete non-judgemental friendship is established, giving the child the feeling they can discuss 'anything'.

5. *Sex talk*. In the final stage, explicit conversations are initiated with the child. Frequently too, the child is asked to supply sexually explicit pictures of themselves. At this stage too, the paedophile will usually try to arrange a meeting with the child.

The offender has a wide range of choice; the means of performing this type of offence are rich and varied. Conventional chat sessions such as MSN and Yahoo Messenger (with or without the use of a webcam) are relatively simple to set up as no 'profile' is required to initiate a chat session. Social networking websites such as www.bebo.com and www.facebook.com generally require the user to create a profile before initiating contact with other users, but the details required

for the profile are usually minimal and easily falsified. The sense of anonymity often experienced by offenders using the internet gives them the confidence to perform actions that they might consider unthinkable in real world. These issues are explored in more detail in Chapter 10.

3.2.4 Mobile phones

Recent advances in mobile phone technology have created mobile phones that include a digital camera. Increased memory capacity, removable memory cards, higher still picture resolution and the ability to store several minutes of video footage inevitably make the mobile phone an attractive and portable option for many people, a few of whom will choose to use it to commit offences.

Guardian news and Media Limited (2007) report a number of teenagers arrested for example, for using mobile phones to take indecent images of other children. The BBC (2007a) reports that a barrister too has fallen foul of this technology by allegedly using a mobile phone camera to take covert pictures of girls on trains.

The act of 'happy slapping' is another example of a modern twist on an old crime, reports Guardian news and Media Limited (2005). This is the act of committing an assault or robbery while an accomplice records the act, often with a mobile phone. Sexual assaults (BBC, 2007e) and even murder (BBC, 2007c) have also been recorded in this manner.

3.3 Forensic examination in practice

The precise procedure used for the examination of a digital device is of vital importance. Aside from the accreditation issues discussed later, there are no nationally agreed standards, rules or protocol for the handling of computer evidence. There are certainly ACPO guidelines for the handling of such evidence, but they are little more than best practice advice.

From a prosecution point of view a forensic examination of a digital device is generally considered to be conducted in four primary stages:

- acquisition;
- identification;
- evaluation; and
- presentation.

The acquisition stage is concerned with the forensically sound capture of the data. A digital device involved in a crime is effectively a crime scene in its own right which needs to be secured, just as much as a murder scene. Like fingerprint and DNA evidence, digital evidence is fragile and easily lost if appropriate precautions are not followed. Horror stories of over-zealous police officers switching on digital cameras to look for evidence or conducting virus scans on floppy disks prior to submitting them for a forensic examination still haunt investigators working in the field. The location in which the exhibit was found and seized is also an important factor to record as it can reveal a great deal about the intent of the suspected offender. For example, was the wireless device hidden beneath floorboards, or was it in an open access area like a living room?

One of the most important aspects of the acquisition stage is the process of forensically copying the data from the digital device onto an 'evidence disk'. The accepted best practice to achieve this is to use a hardware write-blocking device. The device is installed between the evidence disk and the forensic workstation, and only allows data to pass in one direction. It is designed to stop any write signals being passed from the receiving computer back to the evidence disk, hence preserving the data contained on the evidence disk in its original form.

Data recovery from hard drives

Robin Bryant

Digital forensic investigation frequently involves the recovery of digital information from PCs, PDAs, mobile phones, GPS devices and indeed just about any device with electronic memory. Some of these may contain memory in the form of a hard drive and the device may also employ a Windows GUI interface. In terms of digital forensics, files and folders on a hard drive can be thought of as falling into one of four different categories (our terminology):

'Obvious' These are files and folders which are obviously either part of the operating system (e.g. MS Word), or files (such as an MS Word document) which have been saved by a particular program. Some of these are certainly of potential interest to the digital forensic investigator. For example, one useful folder in Windows XP might

be found in the folder C:\Documents and Settings\User\Local Settings\Temporary Internet Files. This folder contains information concerning internet sites visited with dates and times.

'Obscure' These are files and folders which, although not necessarily hidden (by the user or by the default setting of the GUI), do not have an obvious meaning or use. Examples include 'temp' files which may have the format '*.tmp' where * is a wildcard (e.g. ~WRL0554.tmp). For example, when using MS Word, copies of the document are often saved as *.tmp files which can usually be read as a document, by either changing the file extension to 'doc' or by associating MS Word with the file extension. (Although, in practice, an alternative program to the original would probably be used in a forensic investigation to examine the file, in order to avoid modifying the original.)

'Hidden' These are files and folders which, although still present and intact on the hard drive, are hidden from the user. They will not even be revealed by ticking the 'Show hidden files and folders' checkbox within the normal Windows routine.

'Deleted' These are files which have either been deliberately deleted by the user (for example, in Windows, by sending a file to the 'Recycle Bin' and then emptying the bin) or have been automatically deleted, perhaps on booting up. A fundamental premise of the forensic recovery of deleted data is that it is actually surprisingly difficult for a person to completely and irretrievably delete a file. Unless special software is used, or particular command line actions taken, the likelihood is that at least part of the deleted file is actually still present on the hard drive (particularly with more modern PCs with large capacity hard drives).

However, note that there are also other 'file residues' that may be located, such as ambient data, file slack, free space, and shadow data. The 'page file' is possibly the most important type of ambient data. Page files are found with all Windows operating systems as a form of electronic 'scratch pad' to write data when additional random access memory is needed and may contain logon names, passwords and fragments of messages and documents. Most users are unaware of the existence of the page file. Other areas containing file or folder details include registry, thumb.db files, email attachments and event logs.

The recovery of obscure, hidden and deleted files is usually one of the tasks of a digital forensic investigator. As an example consider the forensics of retrieving information concerning a person's use of the internet from an image of their PC's hard drive. Apart from examining obvious and obscure files and folders and attempting the recovery of deleted files, the investigator would also probably access a hidden folder called 'content.ie5' which contains a file called 'index.dat'. This file records information about any websites visited, and (unusually) is not deleted by clearing the temporary internet files from folders. The content of the .ie5 folder and index.dat file will not be made visible using the usual Windows 'Show hidden files and folders' tab. It will be made visible however, by running the command <dir/ a "%Userprofile%\Local Settings\Temporary Internet Files*.*" >. (Dedicated forensically validated software is commercially available for this procedure, and in addition provides a user-friendly interface for collecting the information).

In the identification stage, the precise location of relevant digital data must be established. A computer with two hard disks, for example, can be initially considered at a physical level in terms of a base unit, disk 1 and disk 2. Examples of the properties that are of interest from this perspective are the system date and time on the base unit, the number of sectors on both disks and whether any hidden sectors reside on either disk. At a logical level, the number and type of partitions present, and the type and structure of the file system are also of interest; they may reveal much about the owner's level of knowledge. Finally, the identification stage considers the context within which any evidence is found. A good example of this is when a particular credit card number (significant within an investigation) is found in the area of a hard disk where previous files once resided, known as unallocated clusters. Here, ghosts of former files reside in part or even in full and these may be used to identify the original context of the credit card number; for instance, was the card number in the content of an email? This may be crucial if the evidence is to be exhibited for use in court.

In the evaluation stage a decision on the relevance of the find is made. A clear understanding is required of how the data was produced, when it was produced and by whom. It is at this stage that the common defence of Trojans and pop-ups in internet browsing-related offences can be discounted through the examination of any malware found on the device, live port activity and internet searching habits, for example.

The presentation stage involves the interpretation of the raw data and the reconstruction of events that occurred on the exhibit prior to its seizure. The report must be technically concise, but clearly written for the lay person if it is to be understood by the court. The author of the report must be prepared to be questioned and perhaps even defend their findings in a court of law.

3.3.1 Best practice principles

ACPO have published the *Good Practice Guide* for the recovery of computer-based electronic evidence (Association of Chief Police Officers of England, 2007). In this document they identify four primary guidelines, which we summarise here:

Principle 1: no action taken should change data held on an exhibit.

Principle 2: where a person finds it necessary to access original data held on an exhibit that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3: an audit trail of all processes applied to an exhibit should be created and preserved. This would be repeatable to an independent third party.

Principle 4: the person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

These principles influence many of the procedures followed when examining a digital device. Thus, the acquisition stage must preserve and not alter the state of the exhibit and thereby uphold Principle 1. Under certain circumstances, such as when acquiring data from a corporate server, it is impractical to take the device offline and so data from selected areas of the server must be captured. (Other areas of the server may be inaccessible to the suspect, so are not required for the investigation.) To adhere to Principle 2, the impact of these actions must be known and should only be undertaken by a competent person. When identifying and evaluating evidence a comprehensive set of contemporaneous notes must be made in order to record and document the processing of an exhibit, in accordance with Principle 3.

3.4 Professional accreditation

Digital forensics is a new and developing field, and is increasingly recognised as a scientific discipline in its own right. More and more organisations are offering services, seminars, courses and accreditation in an effort to define and become the *de facto* standard in this specialised market.

This open market approach has led to a number of problems for managers of forensic units and staff, particularly within the court system of England and Wales. First, there is no single and mandatory regulatory body to provide a line of professional accountability for digital forensics specialists. Professional accountability is of vital importance for practitioners, particularly when liaising with other professionals and institutions. Practising lawyers, for example, are answerable to the Bar Standards Board and medical doctors are answerable to the British Medical Association (BMA).

Second, there is no digital forensics professional qualification that is universally recognised as the professional standard. For example, professional engineers are frequently expected to possess Chartered Engineer (CEng) status; this is a recognised standard for engineering, but for digital forensics there are at present two registers (and both are optional), one within the Council for the Registration of Forensic Practitioners and the other being developed by Skills for Justice.

There is also no single nationwide training programme for digital forensics specialists. The implications of this are significant. First, there is no nationally agreed career path for a digital forensic examiner, and therefore no way of establishing that an individual is 'qualified' to practise. Second, there is no 'best practice' or industry standard on how to undertake the various processes used to analyse digital data.

Currently, it is left very much up to the court to accept the credentials and experience of an individual prior to accepting their evidence in court. This can and does lead to a forensic examiner's credibility being challenged in an attempt to have their testimony rejected by the court. The primary cause of this situation is the infancy of the field. From a law enforcement perspective, investigations involving the forensic analysis of computers began around 1997 with Kent Police establishing one of the first hi tech crime units in the country. More recently, the UK's National High-Tech Crime Training Centre (now part of the National Police Improvement Agency, the NPIA) has developed a number of training courses in forensic data investigation and internet investigation (at initial, intermediate and advanced levels) for investigators working both in the UK and further afield. The intention is to develop a common training model for high tech crime investigation

training throughout Europe, and a linked professional register of recognised high tech crime investigators (Bryant and Jones, 2005).

3.4.1 Council for the Registration of Forensic Practitioners

The Council for the Registration of Forensic Practitioners (CRFP) was established in 1999. It is a non-profit making organisation (subsidised by a grant from the Home Office) and is independent of the Government. The Council's remit is to maintain a register of currently competent forensic practitioners and to ensure that registered practitioners stay up to date and maintain their level of competence. Initially, the register only covered the mainstream forensic specialties of science, fingerprints and scene examination, but it has been extended more recently and now includes forensic medicine, road transport investigation and fire-scene examination. Within digital forensics, the CRFP identify three processes; namely:

- Data capture;
- Data examination; and
- Data evaluation.

Data capture is the retrieval of data using forensically sound processes coupled with the creation of systems to verify the data captured. Software products such as Guidance Software's EnCase and Access Data's Forensic Toolkit (FTK) perform these two steps in one process.

The data examination role relates to the identification and examination of relevant data in an investigation. In addition, the CRFP also consider the production of exhibits (to assist the court) to be part of this role.

The data evaluation role encompasses the assessment of data in its context and assesses the significance of the data for the case in question. The forensic practitioner is also equipped to draw deductions from the data and consider alternative hypotheses.

A digital investigator may apply to join the CRFP register. The CRFP application process (at the time of writing) considers the skills of a practitioner in terms of these three roles (data capture, examination and evaluation). The application involves two separate application packs; 'Computer Examination' and 'Computers'. The data capture and examination roles fall under the Computer Examination category, as they are considered to use investigative skills. Data evaluation, which is considered to use higher level skills (similar to the skills possessed by a

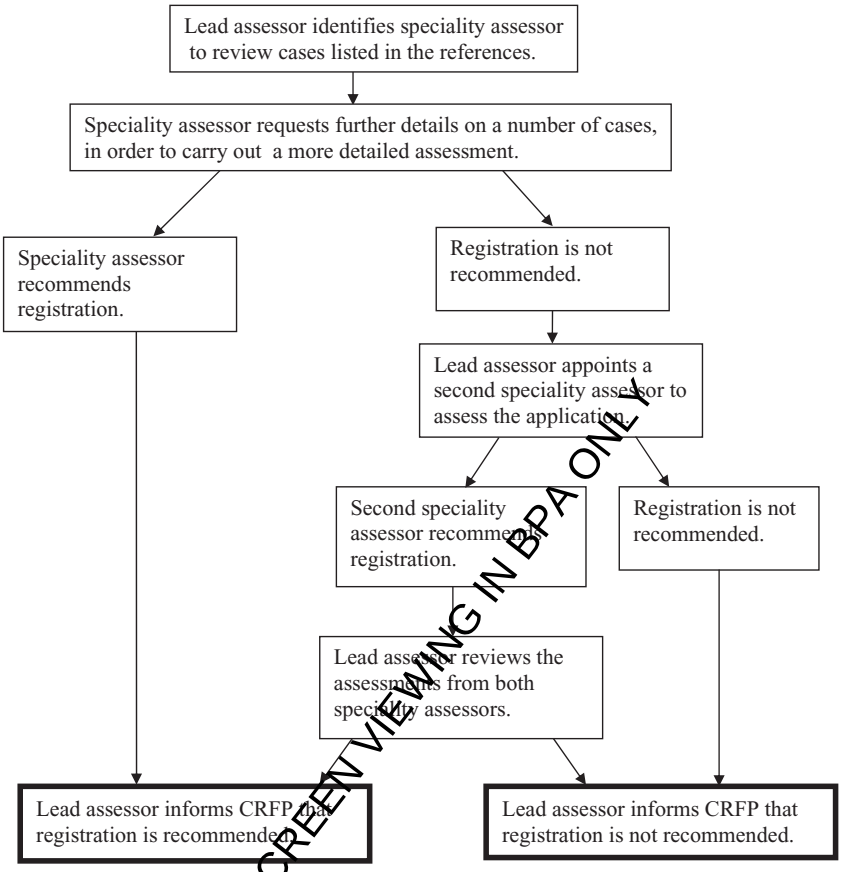

Figure 3.4 Applying for CRFP registration

forensic scientist or an engineer) is covered by the Computers application pack. A forensic examiner who undertakes all three roles (data capture, examination and evaluation) must therefore complete two application packs.

Each application is processed in three stages. In the first stage (Initial Application), the applicant returns the completed application pack(s) to the CRFP, who then obtain the relevant references for the lead assessor. The second and third stages of the application process (Further Information and Final Assessment) are shown in figure 3.4.

A successful applicant will be granted registration for 4 years. After this time has elapsed the renewal of their registration will depend upon their ability to demonstrate that they have remained up to date and maintained their competence.

In addition, the investigator's recent casework will be subjected to a further formal assessment.

Despite being based upon a system of peer review, the Seventh Report by the Select Committee on Science and Technology (Great Britain. House of Commons Science and Technology Select Committee, 2005) identified a number of potential issues with the Register. Under the present system, the discredited expert witness Professor Meadow would probably have had no difficulty in obtaining CRFP registration. Professor Meadow found himself in this situation largely due to the fact that he gave evidence in an area that was not his specialty. Solicitors and policy advisors for the CPS have also voiced concerns over the registration process as it stands, citing that there is no 'remit of evidence-based practice' and that it should not become a 'panacea for exercising a judge's discretion'.

The independent auditing of the assessment processes for granting initial accreditation and renewal of accreditation is called for. But digital forensics is a small field (compared to more established information technology based fields such as Artificial Intelligence or Software Engineering) and so the number of specialists is inevitably small. Independent auditing would consequently be difficult to arrange. As pointed out by the report, for small specialist communities like CRFP, it is inevitable that such a register will have a limited validity; members of such communities are all responsible for accrediting each other.

3.4.2 Skills for Justice

A key remit for the relevant Sector Skills Council, Skills for Justice (SfJ), is the introduction of National Occupational Standards (NOS). These standards measure an individual's competence by assessing performance in terms of nationally agreed outcomes. In terms of the investigation of digital crime, the relevant NOS are to be found within the 'Countering E-Crime' suite of competencies.

The Countering E-Crime NOS introduced by SfJ (after extensive consultation with representative employer organisations) comprises of eight units; two mandatory, one mandatory–optional and five optional.

Mandatory Units

- Identify and secure electronic evidence sources.
- Health and safety in ICT and Contact Centres.

Mandatory-Optional Units (at least one must be completed)

- Seize and record electronic evidence sources.
- Capture and preserve electronic evidence.

Optional Units (at least five must be completed)

- Seize and record electronic evidence sources.
- Capture and preserve electronic evidence.
- Investigate electronic evidence.
- Evaluate and report electronic evidence.
- Conduct internet investigations.
- Conduct network investigations.
- Working with ICT hardware and equipment.
- Technical advice and guidance.
- Security of ICT systems (Skills for Justice, 2007).

The modular, competence based approach to assessment mirrors the foundations of National Vocational Qualifications (NVQs) and Scottish Vocational Qualifications (SVQs). This approach also makes it relatively straightforward to identify areas that need further development. The distinguishing characteristics that define a successful performance (within an established role such as digital forensics) are known as competencies, reports Wolfe (1998). Any combination of knowledge, skill, traits, values/beliefs, motives, and physical ability can be assessed.

Competence based assessment is viewed by many organisations as a more suitable tool to assess workplace skills than traditional academic qualifications alone. Their modular nature makes them scaleable, meaning that as new roles are created within an organisation, appropriate competencies for the new role can be chosen from existing competencies, and additional competencies can be added to distinguish the new role from the existing role(s). Concerns however have been expressed within the academic community concerning the

'box-ticking' nature and general limitations of competencies based learning and assessment.

3.4.3 Models for professional accreditation

There is currently no professional body for digital forensic investigators and allied occupations. The establishment of a mandatory regulatory body, with the authority to issue a license to practise would help define the standards and level of expertise required of a digital forensics specialist, and courts would be likely to have greater confidence in the skills, experience and accountability of an individual specialist. It would seem rational to suppose that such a regulatory body would be led by a single voice. Without clear leadership, it is likely that prolonged debate concerning the mechanisms for arranging peer review would inevitably dilute the credibility of any professional body, defeating its very purpose.

Many professional bodies also have close ties not only with industry, but also with current research and development in order to keep abreast of the latest scientific knowledge and recommendations for best practice. The advantages for a field such as digital forensics are obvious. A regulatory body overseeing digital forensics could also cater for those with and without a higher education; the personnel working in high tech crime units within the police forces of England and Wales comprise of a mixture of both police officers and civilians with a wide range of skills and educational backgrounds.

The fingerprints service might be considered as a possible model for both professional accountability and accreditation within the forensics arena; it might provide a positive role model for other digital forensics specialities. In terms of an individual's professional accountability, fingerprints specialists are regulated by the National Fingerprint Board (NFB) which is made up of senior operational police officers, Home Office representatives and senior forensic practitioners. Standards, performance, training are all areas under the remit of the NFB.

As Mike Thompson, Head of National Fingerprint Training for Centrex (now NPIA) describes (BBC, 2006), the NFB is a regulatory body that has a mandate to enforce compliance throughout the service. A prospective fingerprint expert can expect their training to be evaluated and assessed to ensure that competence is fully proven before they can be recognised and registered as an expert. There is an ongoing process of continuous improvement and development and regular competence testing to demonstrate continuing practical competence on the part of the practitioner.

Digital Forensic Investigation

Robin Bryant

Investigating digital crime does not, of itself, mean that a digital forensic investigation will be undertaken. Some digital crimes, such as identity fraud where the suspect uses the internet as a source of information and a means to commit the crime, could feasibly be investigated entirely successfully using traditional and well established investigative techniques. However, many digital crimes also require a specialised and parallel form of digital forensic investigation. (We use the word 'forensic' here beyond its normal meaning of 'pertaining to the courts' to embrace a wider sense of scientifically-based methodologies).

The diagram below illustrates both some of the usual components of digital forensic investigation (shown in shaded boxes) although by no means all will be used in any particular investigation, together with some indication of investigative methods that span two or more subfields.

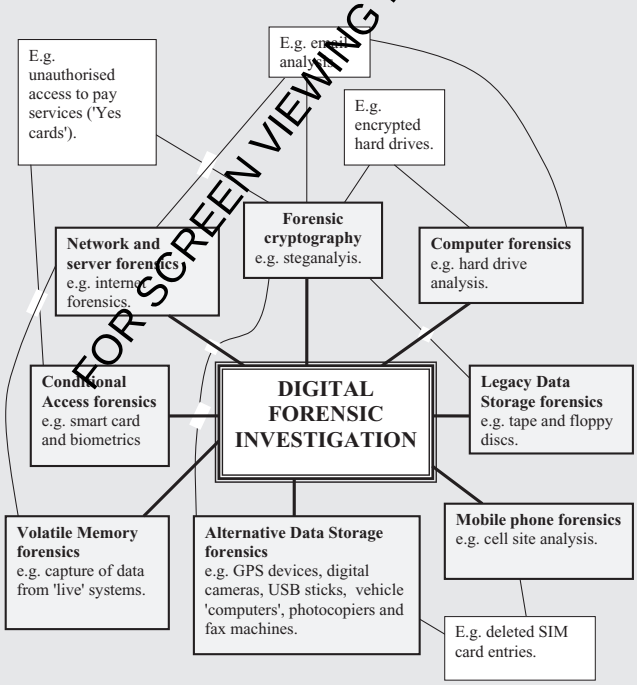

Figure 3.5 Specialist fields within digital forensic investigation

The credibility of a digital forensic analyst needs to be proven and less open to challenge, particularly given the weight that can be placed upon the digital evidence by the courts. Mechanisms need to be put in place for the review of the practices, procedures and performance for the field of study covered by a particular digital forensic analyst. In addition, the training of staff and the maintaining of standards should be demonstrable; a mandatory regulatory body could provide such mechanisms.

3.5 Digital evidence in the courts

The Office of Science and Technology states that any technical process applied to digital evidence 'does not have to pass any formal test' for it to be placed before a court (Great Britain. Parliamentary Office of Science and Technology, 2005). This may seem alarmingly imprecise, but it has certain advantages; a trial judge has the power to admit or decline a particular piece of evidence, and this flexibility allows a court to take advantage of the very latest developments in the digital forensics field.

3.5.1 Presenting digital evidence in court

The Forensic Examiner prepares a statement which is submitted to the Crown Prosecution Service (CPS), and copies are distributed to both the prosecution and defence counsel. The statement explains the examiner's findings and proposes a variety of strategies and the legal points to prove. It should not be just an unbiased and technically accurate document describing the outcome of a forensic examination; explanation and guidance should also be provided, in terms which are comprehensible to the court and witnesses.

The Forensic Examiner's primary role (as for most witnesses summoned to a court within England and Wales) is to assist the court. However, given both the technical complexity of the evidence and the examiner's level of expertise and experience, they are also frequently called upon to interpret the evidence. As Johnston and Hutton (2004) point out, the primary purpose of the statement is to assist the court in evaluating the admissibility and weight of any evidence found on the digital devices examined for the case.

Arguably the most important area to cover when presenting digital evidence to a court is that of continuity. It is absolutely critical to be able to account for what happened to an exhibit such as a computer from the moment it was

seized to the moment it was examined by a forensic examiner. Any gaps in this chain of evidence could mean that one or more unknown persons could have had access to the exhibit and thus have potentially interfered with its integrity. Such discrepancies provide an easy target for defence counsel to discredit the evidence.

Under UK Law each offence has what are known as 'points to prove'. For example, under s 3 of the Computer Misuse Act 1990 a person is guilty of unauthorised modification of computer material if it can be proven that he or she:

(a) does any act which causes an unauthorised modification of the contents of any computer; and

(b) at the time when the act was performed he or she has the requisite intent and the requisite knowledge to do so.

These two points demonstrate what in legal terms is called the *actus reus* (guilty act) and the *mens rea* (intent/knowledge) of the individual.

If the evidence submitted by a digital forensics examiner is unclear or is contradicted by other evidence, the court may move to reject the examiner's evidence. R. v. Cannings (2004) (which passed judgement on Angela Canning's successful appeal against her conviction for murdering her two baby sons) it was stated that 'If the outcome of the trial depends exclusively, or almost exclusively, on a serious disagreement between distinguished and reputable experts, it will often be unwise, and therefore unsafe to proceed' (R. v. Cannings [2004] 1 All E. R. 725).

3.5.2 Interpretation of evidence by a jury

The jury hear first the evidence of the forensic examiner as interpreted by the prosecution counsel, so it is vital that the counsel has a clear understanding of the evidence, and can communicate the key points to the jury effectively. Thus it is essential for the forensic examiner to liaise with the prosecution counsel prior to going to court, in order to check their interpretation of the facts. Such meetings, when they occur, usually take place just prior to going into court, and often only an hour at most after the prosecutor has first seen the digital forensic examiner's statement. Where appropriate, counsel is offered a carefully selected analogy to assist in the comprehension of such data.

There is a school of thought that the juries in cases involving complex digital evidence should be selected from among suitable technically qualified people. The

British Computer Society (2000) proposed this measure in a submission paper. Such a radical measure would need careful consideration as to a suitable means of establishing the degree to which a jury (under the current system) understood and appreciated the significance of evidence concerning digital devices or processes. However, conducting such research inevitably presents difficulties, as identified by section 7 of a report by the House of Commons Science and Technology Select Committee (2005) which states that 'section 8 of the Contempt of Court Act 1981 and the related common law assures the confidentiality of a jury's deliberations and precludes research into these deliberations' (Great Britain. House of Commons Science and Technology Select Committee, 2005, para 164).

3.5.3 Countering a defence

One of the responsibilities of the digital forensic examiner on the prosecution team is to identify and evaluate possible areas of defence that may arise. Probably the most common defence identified at the police interview stage of an investigation is that of a Trojan or 'pop-up' being responsible for the presence of any illegal material on the computer in question. Kennedy (2006) discusses a process that may be followed to investigate the presence and impact of malware.

In some situations a defendant may assert that evidence found on their computer was unsolicited and was 'pushed' to them via MSN, a peer-to-peer application such as Kazaa (or a BitTorrent client) or perhaps by email. These scenarios can be substantiated or refuted through investigation of the computer and how it has been used. Similar techniques can be applied to investigate claims of 'curiosity' when for example, indecent images of children are found on a computer.

The defence may argue that proper procedures have not been followed; procedure is important and must be strictly followed during a digital forensic examination. By keeping contemporaneous notes of all actions performed (particularly in relation to the technical processes followed) it is possible to demonstrate that an empirical approach has been taken to the examination of an exhibit and data contained within it. Although such notes will not find their way into a statement in their entirety they should include any areas of the ACPO guidelines that might need to be evidenced. Thus, when capturing a forensic copy of a hard disk for example, it should be recorded that the process was performed using a hardware write blocking device, and ideally record the device's manufacturer, model and serial number.

If there is a significant difference between the total number of sectors on a hard disk indicated by the label and the number of sectors reported by the analysis tool,

an explanation for this difference should be provided in the statement. Without this the defence could argue that the evidence that vindicates their client is located in this 'missing' area.

3.6 Ethical issues

Digital forensics practitioners (unlike many generalist practitioners) possess the skills to access areas of a hard disk normally hidden to the other users, and this may present ethical dilemmas that can prove difficult to navigate. For example, whilst working on a high profile case a practitioner may be subject to peer pressure to release personal details of the offender to police colleagues and other investigators. The privacy of the offender or client must be maintained in exactly the same way a GP maintains the privacy of a patient, reports ComputerForensics1 (2006). For example, if a hard disk from a lawyer's office is being examined, any records of communications between the lawyer and the client are subject to what is known as 'legal privilege'. This means that such communications are regarded as confidential and must not even be examined, let alone used evidentially by a digital forensics practitioner. These privacy issues can be difficult to untangle at times as it is not always possible to confine an investigation to just one individual. For example, log files or emails between parties will by their very nature contain details such as access times and e-mail accounts of innocent third parties.

It is not difficult to see that, like a locksmith, the digital forensic practitioner's skills can be put to misuse. In privately owned companies the use and misuse of such skills becomes more significant, reports Stahl (2006). Employers may naturally desire information about their employees, and a digital forensics practitioner may be under immense pressure to reveal particular details stored in a digital evidence source. A practitioner who submits to such pressure may stray into the realm of surveillance in the workplace; this is explored in some depth by Stahl *et al*. (2005).

Ethical issues should be explored alongside the provision of ethical guidance during the education and training of a practitioner, but it is not enough to simply 'bolt on' an extra subject to be covered within a digital forensics training programme. The bolt-on approach has the effect of isolating the principles, and seems to imply that it might be optional for the individual to take the concepts on board. Erbacher and Swart (2002) argue that changes in attitude such as ethics are best brought about by regularly integrating ethical considerations and discussions into all aspects of the specialty as a whole.

3.7 Professional development for digital forensics

Establishing digital forensics as a profession is an area explored by Stahl (2006), and would, Stahl asserts, provide guidance for members in the principles upheld by the profession, including ethics. As a professional body, a code of conduct can be established that embodies the expected behaviour of the profession in relation to third parties. This reduces pressure on individuals to behave in way they feel violates the principles upheld by the profession.

Stahl (2006) goes on to point out that, traditionally, members of a profession such as medicine and law are known and respected for their independence and autonomy. Employees within the newer professions such as the various flavours of information communications technology are typically employed by large commercial organisations. In these circumstances, the ethical priorities of the profession inevitably compete with the commercial priorities of the organisation. When a conflict of interest occurs it is likely the professional requirements will take second place to the commercial requirements.

The digital forensics practitioner must reflect upon the position they hold in society; they are in positions of considerable trust and power. For those working in law enforcement, there are times when the reputation and very liberty of people under investigation can depend solely upon the findings of the practitioner's examination.

Questions

Robin Bryant & Sarah Bryant

1. What is 'volatile memory'? How can the forensic 'capture' of the remains of volatile memory be reconciled with current good practice guidelines for the 'first responder'? (Compare the 'safe shutdown school' with the 'live analysis school').

2. What is a 'session cookie' and why might they be of interest to a forensic investigator?

3. In a criminal case, how could the 'trojan defence' be rebutted?

4. Describe how digital technology may contribute to the commission of a 419 scam.

5. What is the system for validating digital forensic software tools in (a) the UK, (b) the US?

6. Why might it be important to use a write blocking device in the course of a digital investigation?

7. What information is stored in a file called 'index.dat' on a PC (as used by the Microsoft web browser Internet Explorer)? Why might this information be of forensic interest?

8. What are the four principles ACPO recommends for any digital investigation?

References

Association of Chief Police Officers of England (2007) Good Practice Guide for Computer-Based Evidence. [Online]. Available at: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf (Accessed: Oct 9 2007).

BBC (2006) Q and A: The fingerprint expert. BBC News [Online]. Available at: http://news.bbc.co.uk/1/hi/programmes/panorama/5007820.stm (Accessed: Sep 9 2007).

BBC (2007a) Lawyer 'stored indecent images'. BBC News [Online]. Available at: http://news.bbc.co.uk/1/hi/england/4930898.stm (Accessed: Sep 14 2007).

BBC (2007b) Identity ring members sentenced. BBC News [Online]. Available at: http://news.bbc.co.uk/1/hi/england/london/6653727.stm (Accessed: Sep 12 2007).

BBC (2007c) Life for 'happy slap' murder boy. BBC News [Online]. Available at: http://news.bbc.co.uk/1/hi/england/southern_counties/6303599.stm (Accessed: Sep 16 2007).

BBC (2007d) Man arrested over Wi-Fi 'theft'. BBC News [Online]. Available at: http://news.bbc.co.uk/1/hi/england/london/6958429.stm (Accessed: Sep 17 2007).

BBC (2007e) Sex attack phone girls detained. BBC News [Online]. Available at: http://news.bbc.co.uk/1/hi/england/london/6970516.stm (Accessed: Sep 16 2007).

BBC (2007f) Sister jailed for identity theft. BBC News [Online]. Available at: http://news.bbc.co.uk/1/hi/scotland/edinburgh_and_east/6969221.stm (Accessed: 12 Sep 2007).

BBC (2007g) Trial hears from Special Branch. BBC News [Online]. Available at: http://news.bbc.co.uk/1/hi/scotland/tayside_and_central/6966846.stm (Accessed: Sep 6 2007).

BBC (2007h) Tutor sent to jail over ID fraud. BBC News [Online]. Available at: http://news.bbc.co.uk/1/hi/wales/south_east/6917965.stm (Accessed: 12 Sep 2007).

British Computer Society (2000) Expert Panels: Legal Affairs Expert Panel, Submission to the Criminal Courts Review, Lord Justice Auld. [Online]. Available at: http://

www.computerevidence.co.uk/Papers/LJAuld/BCSComputerEvidenceSubmission.htm (Accessed: Sep 25 2007)

Bryant, R. and Jones, N. (2005) *Cybercrime Investigation – Developing an International Training Programme for the Future.* Bedford: NSLEC Centre for National High-Tech Crime Training.

ComputerForensics1 (2006) Computer forensic ethics. [Online]. Available at: http://www.computerforensics1.com/computer-forensic-ethics.html (Accessed: Sep 10 2007).

Dhamija, R., Tygar, J.D. and Hearst, M. (2006) Why phishing works. In: Grinter, R. E., Rodden, T., Aoki, P.M., Cutrell, E., Jeffries, R. and Olson, G.M. (eds.) Proceedings of the 2006 Conference on Human Factors in Computing Systems, CHI 2006, Montréal, Québec, Canada: CHI, pp. 581–590.

Erbacher, R.F. and Swart, R.S. (2002) *Computer forensics: training and education*. [Online]. Available at: http://www.cs.usu.edu/~erbacher/publications/ForensicsEducationPaperrevised.pdf (Accessed: Sep 10 2007).

Garlik Limited (2007) UK Cybercrime report. [Online]. Available at: https://www.garlik.com/press/Garlik_UK_Cybercrime_Report.pdf (Accessed: Sep 11 2007).

Great Britain. House of Commons Science and Technology Select Committee (2005) Science and Technology – Seventh Report: (Chapter 7 Use of Forensic Evidence in Court), London: HMSO. [Online]. Available at: http://www.publications.parliament.uk/pa/cm200405/cmselect/cmsctech/96/9610.htm (Accessed: Sep 9 2007).

Great Britain. Office of Public Sector Information (2006) Explanatory Notes to Fraud Act 2006. London: HMSO. [Online]. Available at: http://www.opsi.gov.uk/ACTS/en2006/2006en35.htm (Accessed: 03 Sep 2007).

Great Britain. Parliamentary Office of Science and Technology (2005) Postnote – Science in Court. [Online]. Available at: http://www.parliament.uk/documents/upload/postpn248.pdf#search=%22presenting%20digital%20evidence%20court%22 (Accessed: 26 Sep 2006).

Guardian news and Media Limited (2005) Concern over rise of 'happy slapping' craze. [Online]. Available at: http://www.guardian.co.uk/mobile/article/0,2763,1470214,00.html (Accessed: Sep 16 2007).

Guardian news and Media Limited (2007) Love in the time of phone porn. [Online]. Available at: http://education.guardian.co.uk/sexeducation/story/0,,2001374,00.html (Accessed: Sep 14 2007).

International Centre for Nigerian Law (2007) Criminal code act part VI. [Online]. Available at: http://www.nigeria-law.org/Criminal%20Code%20Act-Part%20VI%20%20to%20the%20end.htm (Accessed: 3 Sep 2007).

Johnston, D. and Hutton, G. (2004) *Blackstone's Police Manual, Evidence and Procedure*. Oxford: Oxford University Press, p. 133.

Kennedy, I.M. (2006) It was a big wooden horse, your Honour. [Online]. Available at: http://www.bcs.org/server.php?show=ConWebDoc.6232 (Accessed: Sep 27 2006).

O'Connell, R. (2007) A typology of child cybersexploitation and online grooming practices. Lancashire: University of Central Lancashire, 24 July 2003, [Online]. Available at: http://www.uclan.ac.uk/host/cru/docs/cru010.pdf (Accessed: Sep 24 2007).

Skills for Justice (2007) National Occupational Standards for the Justice Sector. [Online]. Available at: http://www.skillsforjustice.com/nos/with-ple.htm (Accessed 10 Oct 2007).

Stahl, B.C. (2006) Is forensic computing a profession? Revisiting an old debate in a new field. *Journal of Digital Forensics, Security and Law,* **1**(4):49–66 [Online]. Available at: http://www.cse.dmu.ac.uk/∼bstahl/publications/2006_forensic_computing_profession_JDFSL.pdf (Accessed: Sep 10 2007).

Stahl, B.C., Prior, M., Wilford, S. and Dervla, C. (2005) Electronic monitoring in the workplace: if people don't care, then what is the relevance? In: Weckert, J. (ed.) *Electronic Monitoring in the Workplace: Controversies and Solutions*. USA: Idea-Group Publishing, pp. 50–78.

Symantec Corporation (2007a) A Monster Trojan. [Online]. Available at: http://www.symantec.com/enterprise/security_response/weblog/2007/08/a_monster_trojan.html (Accessed: Sep 12 2007).

Symantec Corporation (2007b) Symantec Internet Security Threat Report. [Online]. Available at:http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-white-paper_internet_security_threat_report_xii_09_2007.en-us.pdf (Accessed: Sep 17 2007).

Thornton, J. (1997) The general assumptions and rationale of forensic identification. In: Faigman, D.L., Kaye, D.H., Saks, M.J. and Sanders, J. (eds.) *Modern Scientific Evidence: The Law And Science Of Expert Testimony* **2**. St. Paul: West Publishing Co.

Wolfe, M. (1998) Transitioning to a competency pay system. *Conference Proceedings of Linkage Incorporated, USA* **5**:203–279.